(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 October 2003 (30.10.2003)

PCT

(10) International Publication Number
WO 2003/090046 A3

(51) International Patent Classification[7]: G06F 1/00, 21/00

(21) International Application Number:
PCT/GB2003/001466

(22) International Filing Date: 2 April 2003 (02.04.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0208916.7 18 April 2002 (18.04.2002) GB

(71) Applicant *(for all designated States except US)*: **ISIS INNOVATION LIMITED** [GB/GB]; Ewert House, Ewert Place, Summertown, Oxford OX2 7SG (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HEASMAN, John** [GB/GB]; 4, Surrey View, Roundabout Road, Copthorne, Crawley RH10 3LD (GB). **MOYLE, Steve** [GB/GB]; 1, Summerfield Road, New Hinksey OX1 4RU (GB).

(74) Agent: **STRACHAN, Victoria, Jane**; Urquhart-Dykes & Lord, Alexandra House, 1 Alexandra Road, Swansea SA1 5ED (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

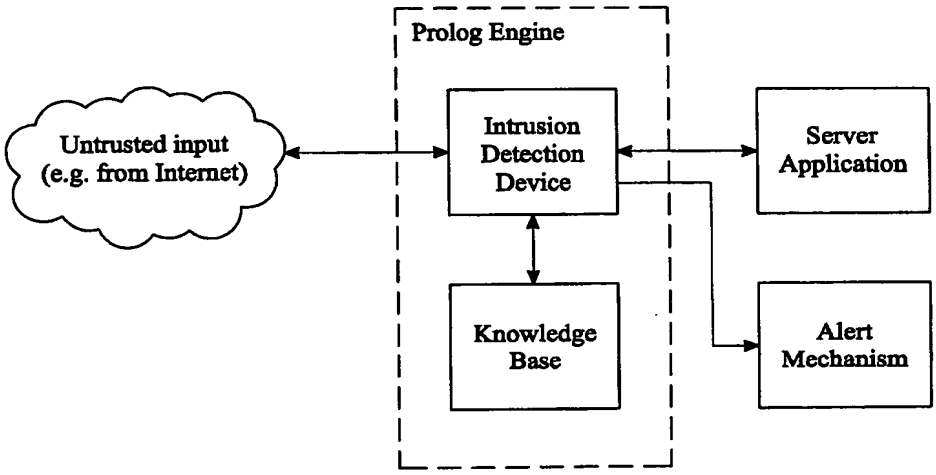
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
29 April 2004

[Continued on next page]

(54) Title: INTRUSION DETECTION SYSTEM



(57) Abstract: An intrusion detection system for detection of intrusion or attempted intrusion by an unauthorised party or entity to a computer system or network, the intrusion detection system comprising means for monitoring the activity relative to the computer system or network, means for receiving and storing one or more general rules, each of the general rules being representative of characteristics associated with a plurality of specific instances of intrusion or attempted intrusion, and matching means for receiving data relating to activity relative to said computer system or network from the monitoring means and for comparing, in a semantic manner, sets of actions forming the activity against the one or more general rules to identify an intrusion or attempted intrusion. Inductive logic techniques are proposed for suggesting new intrusion detection rules for inclusion into the system, based on examples of sinister traffic.

WO 2003/090046 A3

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

PCT/GB 03/01466

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DEBAR H ET AL: "A REVISED TAXONOMY FOR INTRUSION-DETECTION SYSTEMS" ANNALES DES TELECOMMUNICATIONS - ANNALS OF TELECOMMUNICATIONS, PRESSES POLYTECHNIQUES ET UNIVERSITAIRES ROMANDES, LAUSANNE, CH, vol. 55, no. 7/8, July 2000 (2000-07), pages 361-378, XP000954771 ISSN: 0003-4347	1,4
Y	page 362, left-hand column, paragraph II.2 page 364, left-hand column, paragraph IV.1.1.	2,3,5-7

-/--

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 February 2004	01/03/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Arbutina, L

INTERNATIONAL SEARCH REPORT

PCT/GB 03/01466

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	LEE W ET AL: "A FRAMEWORK FOR CONSTRUCTING FEATURES AND MODELS FOR INTRUSION DETECTION SYSTEMS" ACM TRANSACTIONS ON INFORMATION AND SYSTEM SECURITY, ACM, NEW YORK, NY, US, vol. 3, no. 4, November 2000 (2000-11), pages 227-261, XP001078157 ISSN: 1094-9224 abstract page 228, paragraph 1 -page 239, paragraph 4.3 ---	2,3,5-7
X	KO C: "Logic induction of valid behavior specifications for intrusion detection" SECURITY AND PRIVACY, 2000. S&P 2000. PROCEEDINGS. 2000 IEEE SYMPOSIUM ON BERKELEY, CA, USA 14-17 MAY 2000, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 14 May 2000 (2000-05-14), pages 142-153, XP010501131 ISBN: 0-7695-0665-8 the whole document ---	1-8
X	LUNT T F ET AL: "KNOWLEDGE-BASED INTRUSION DETECTION" PROCEEDINGS OF THE ANNUAL ARTIFICIAL INTELLIGENCE SYSTEMS IN GOVERNMENT CONFERENCE. WASHINGTON, MAR. 27 - 31, 1989, WASHINGTON, IEEE COMP. SOC. PRESS, US, vol. CONF. 4, 27 March 1989 (1989-03-27), pages 102-107, XP000040018 page 103, paragraph 3 page 104, paragraph 5 ---	1
X	LINDQVIST U ET AL: "DETECTING COMPUTER AND NETWORK MISUSE THROUGH THE PRODUCTION-BASED EXPERT SYSTEM TOOLSET (P-BEST)" PROCEEDINGS OF THE 1999 IEEE SYMPOSIUM ON SECURITY AND PRIVACY. OAKLAND, CA, MAY 9 - 12, 1999, PROCEEDINGS OF THE IEEE SYMPOSIUM ON SECURITY AND PRIVACY, LOS ALAMITOS, CA: IEEE COMP. SOC, US, 9 May 1999 (1999-05-09), pages 146-161, XP000871982 ISBN: 0-7695-0177-X page 146, paragraph 1 -page 150, left-hand column, last line --- -/--	1

INTERNATIONAL SEARCH REPORT

PCT/GB 03/01466

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KORAL ILGUN: "USTAT: A REAL-TIME INTRUSION DETECTION SYSTEM FOR UNIX" PROCEEDINGS OF THE COMPUTER SCOIETY SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY. OAKLAND, MAY 24 - 26, 1993, PROCEEDINGS OF THE COMPUTER SOCIETY SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY, LOS ALAMITOS, IEEE COMP. SOC. PRESS, US, vol. SYMP. 14, 24 May 1993 (1993-05-24), pages 16-28, XP000416058 the whole document	1
A	SINCLAIR; PIERCE; MATZNER: "An application of Machine Learning to Network Intrusion Detection" INTERNET, RETRIEVED ON 09.02.2004, 1999, XP002269870 Proceedings of 15th Annual Computer Security Applications Conference Dec.1999 the whole document	